

United States District Court  
for the  
Western District of New York

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address.)

INFORMATION ASSOCIATED WITH EMAIL ACCOUNT  
dking\_3@hotmail.com AND USERNAMES dking\_3, dflores93, and  
dfloresart, STORED AT PREMISES OWNED, MAINTAINED,  
CONTROLLED, OR OPERATED BY THE INTERNET SERVICE  
PROVIDER KNOWN AS MICROSOFT CORPORATION

Case No. 18-MJ-1095-2

1096 JJM  
JTB

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Email account dking\_3@hotmail.com and usernames dking\_3, dflores93, and dfloresart

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment D, Description of Items to be Seized.

The basis for search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of Title 18, United States Code, Sections 2251, 2252A(a)(2)(A), and 2252A(a)(5)(B).

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

JUSTIN J. BURNHAM  
SPECIAL AGENT  
HOMELAND SECURITY INVESTIGATIONS  
Printed name and title

Sworn to before me and signed in my presence.

Date: July 16, 2018

  
Judge's signature

City and state: Buffalo, New York

JEREMIAH J. MCCARTHY  
UNITED STATES MAGISTRATE JUDGE  
Printed name and Title

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

STATE OF NEW YORK     )  
COUNTY OF ERIE         )  
CITY OF BUFFALO        )

Justin J. Burnham, being duly sworn, deposes and states:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with Homeland Security Investigations (HSI) and have been so employed since October of 2008. I am currently assigned to the Buffalo Field Office of HSI and I am assigned to the Child Exploitation Unit (CEU). As a member of the CEU, I investigate the sexual exploitation of children, including possession, receipt, and the production of child pornography, as well as coercion and enticement, in violation of Title 18, United States Code, Sections 2251, 2252, 2252A, and 2422(b). I have received specialized training in the area of child pornography, child exploitation, and coercion and enticement, and I have had the opportunity to observe and review numerous examples of child pornography, as defined in Title 18 United States Code, Section 2256.

2. I make this affidavit in support of an application for search warrants for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by three providers:

- a. Google, Inc. (Hangout, Gmail)
- b. Microsoft Corporation (Skype, Hotmail)
- c. Tumblr, Inc.

3. Google, Inc. is headquartered at 1600 Amphitheatre Parkway in Mountain View, California 94043.

4. Microsoft Corporation is headquartered at 1 Microsoft Way in Redwood, Washington 98052.

5. Tumblr Inc., is headquartered at 35 East 21<sup>st</sup> Street, Ground Floor in New York, New York 10010.

6. I make this affidavit in support of an application for a search warrant for information associated with:

a. Two (2) Google, Inc. accounts, [Parrotart2012@gmail.com](mailto:Parrotart2012@gmail.com) and the Google account associated with Google Voice telephone number (716) 467-2535, as identified and described in the following paragraphs and in Attachment A;

b. Three Microsoft Corporation accounts, two (2) of which are the Skype accounts of dflores93 and dfloresart, and the other is the Hotmail account of [dking\\_3@hotmail.com](mailto:dking_3@hotmail.com) as identified and described in the following paragraphs and in Attachment C; and

c. One (1) Tumblr, Inc. account, “dflo93”, as identified and described in the following paragraphs and in Attachment E.

7. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Microsoft Corporation, and Tumblr, Inc. to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Google, Skype, Hotmail, and Tumblr accounts, herein "SUBJECT ACCOUNTS" listed in paragraphs 6a, 6b, and 6c above.

8. As set forth below there is probable cause to believe that evidence, contraband, fruits and instrumentalities of violations of Title 18, United States Code, Section 2251 (production of child pornography), Title 18, United States Code, Section 2252A(a)(2)(A) (receipt and distribution of child pornography), and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography), are located within the SUBJECT ACCOUNTS. There is also probable cause to search the information described in Attachment A, Attachment C, and Attachment E for evidence, instrumentalities, contraband, and fruits of these crimes as further described in Attachment B, Attachment D, and Attachment F.

9. The statements contained in this affidavit are based upon my investigation, information provided to me by other law enforcement personnel, and on my experience and training as a Special Agent of HSI. Because this affidavit is being submitted for the limited purpose of establishing probable cause to secure a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18,

United States Code, Section 2251, Title 18, United States Code, Section 2252A(a)(2)(A), and Title 18, United States Code, Section 2252A(a)(5)(B) are presently located in the SUBJECT ACCOUNTS.

**APPLICABLE LAW**

10. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, enticing, or coercing any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

b. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving, distributing, or conspiring to receive or distribute, or attempting to do so, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

c. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

### **DEFINITIONS**

11. The following definitions apply to this Affidavit and Attachments B, D, and F:

a. “Child Pornography” is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has

been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

b. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

c. “Minor” means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

d. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

e. “Computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1).

f. “Computer hardware” consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices), peripheral

input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. “Computer software” is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic or other digital form. It commonly includes computer operating systems, applications and utilities.

h. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software or other related items.

i. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to unlock particular data security devices. Data security hardware may include encryption devices, chips and circuit boards. Data security software of digital code may include programming code that creates test keys or hot keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or booby-trap protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.



j. “Internet Service Providers or ISPs” are commercial organizations, which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or coaxial cable data transmission, dedicated circuits or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a coaxial cable system, and can access the Internet by using his or her account name and password.

k. “ISP Records” are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP’s servers and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers use. This

service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

l. “Internet Protocol address or IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a subscriber’s computer at varying intervals at the discretion of the ISP. IP addresses might also be static meaning an ISP assigns a user’s computer a specific IP address which is used each time the computer accesses the Internet.

m. The terms “records”, “documents”, and “materials” include all information recorded in any form, visual or aural, and by any means, whether in hand-made form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, printing and/or typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

n. “Image or copy” refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device.

Imaging or copying maintains contents, but attributes may change during the reproduction.

o. “Hash value” refers to a value generated after data has been subjected to a cryptographic mathematical algorithm. A hash value is akin to a digital fingerprint in that dissimilar data will not produce the same hash value after being subjected to the same hash algorithm. Therefore, a hash value is particular to the data from which the hash value was generated. Known hash values can be used to search for identical data stored on various digital devices and/or media as identical data will have the same hash value.

p. “Compressed file” refers to a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

#### **STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS**

12. Pursuant to Title 18, United States Code, Section 2703(b), the contents of an electronic communication that is in electronic storage in an electronic communications system for more than 180 days may be obtained “pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with *jurisdiction over the offense under investigation...*” (emphasis added). Further, pursuant to Title 18, United States Code, Section 2703(b)(1)(A), where such a warrant is obtained, no notice to the subscriber or customer is required to be given.

13. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States...that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

#### **A. Investigation:**

14. On or about December 21, 2017, Microsoft Corporation submitted CyberTipline Report numbers 26299975 and 26300934 to NCMEC regarding the possession of child pornography by a suspect with the Skype username of “dfloresart” who used the IP address of 76.180.3.106 on two occasions on December 16, 2017 to upload child pornography. The image associated with CyberTipline Report number 26299975 included an Electronic Service Provider (ESP) content rating of A2, which is defined as “Prepubescent Minor” and “Lascivious Exhibition.” The image associated with CyberTipline Report number 26300934 included an ESP content rating of B2, which is defined as “Pubescent Minor” and “Lascivious Exhibition.” A NCMEC analyst also viewed the images and found them to contain “Apparent Child Pornography”.

15. On or about December 23, 2017, Google, Inc. submitted Cybertip number 26337032 to NCMEC regarding the possible possession of child pornography by a suspect with the telephone number (716) 467-2535 and email address of [Parrotart2012@gmail.com](mailto:Parrotart2012@gmail.com)

and secondary email address of dking\_3@hotmail.com who used the IP address of 2604:6000:7b01:400:3849:c16e:8975:575c on December 21, 2017 at 11:17:14 UTC to upload said child pornography.

16. On January 4, 2018, Cybertip 26337032 was reviewed by the New York State Police (hereinafter "NYSP"). The image depicts a naked prepubescent male child who appears to be under 8 years of age. The child is observed lying on his back with his legs spread apart, exposing his penis and anus in a lewd manner.

17. On January 19, 2018, a DHS administrative summons was sent to Verizon Wireless for information associated with telephone number (716) 467-2535.

18. On January 29, 2018, Verizon Wireless responded to the summons by providing the following information, among other information:

Customer Name:	Jose Perez
Customer Address:	131 West 2 <sup>nd</sup> Street, Dunkirk, New York 14048
Telephone:	(914) 648-8134

19. On January 29, 2018, a DHS administrative summons was sent to Charter Communications, Inc. for information associated with the upload IP address of: "2604:6000:7b01:400:3849:c16e:8975:575c on December 21, 2017 at 11:17:14 UTC."

20. On January 30, 2018, Charter Communications responded to the summons by providing the following information, among other information:

Customer Name:	Jose Perez
Account Address:	131 West 2 <sup>nd</sup> Street, Dunkirk, New York, 14048
Telephone:	(914) 648-8134

21. On June 1, 2018, the NYSP applied for and received a New York State (NYS) search warrant authorizing the search of the premises located at 131 West 2<sup>nd</sup> Street in Dunkirk, New York.

22. On June 5, 2018, the NYSP with assistance from the Homeland Security Investigations (HSI) Child Exploitation Unit (CEU), executed the NYS search warrant at 131 West 2<sup>nd</sup> Street in Dunkirk, New York. During the search warrant, multiple items were seized, including two cellular telephones found in FLORES' bedroom.

**B. Interview with the Defendant:**

23. Consensual, non-custodial, post-Miranda interviews, including a polygraph interview, were conducted with FLORES on June 5, 2008. During these interviews, FLORES admitted that the recovered cellular telephones belonged to him and that he had previously used them to produce, distribute, receive, and possess child pornography.

24. During these interviews, FLORES admitted he used the services of social media companies to possess, receive, and distribute child pornography. More specifically,

FLORES advised he used the Google, Inc. accounts of [Parrotart2012@gmail.com](mailto:Parrotart2012@gmail.com) and the Google account associated with Google Voice telephone number (716) 467-2535, the Microsoft Corporation e-mail account of [dking\\_3@hotmail.com](mailto:dking_3@hotmail.com) and the Skype accounts of “dflores93” and “dfloresart”, as well as the Tumblr, Inc. account of “dflo93” to distribute, receive, and possess child pornography. FLORES further admitted he has been using the telephone number of (716) 467-2535 with his two cellular telephones for the past five (5) years.

25. FLORES said he was first introduced to child pornography approximately 1 – 1.5 years ago through an individual from Pennsylvania he met on a dating application. FLORES said they met on the social media application, KIK, where they chatted. FLORES said this man knew of a KIK group chat and sent him an invitation to join the group. FLORES said the group consisted of approximately 9 to 10 people and that these individuals “made” him the head of the group. FLORES said it wasn’t long before his KIK account was then suspended. FLORES said that members of this group would send child pornography to each other, that he received child pornography from members of this group, and that he has sent child pornography to them as well. FLORES said he would also “role-play” with the members of this group. When asked to describe the child pornography that was distributed in this group, FLORES said the pictures were of men and kids having sex with each other. Flores said he enjoyed satisfying the needs of these men.

26. During the June 5, 2018 interview, FLORES also stated that he engaged in sexual contact with multiple individuals who were under the age of eighteen years of age.

**c. Minor Victim 1:**

27. During the interviews, FLORES admitted he had sexual contact with a fourteen-year-old boy, herein minor victim 1 (MV1). The identity of MV1 is known, but is being redacted because he is a minor. When asked to describe the sexual contact with MV1, FLORES admitted he and MV1 touched each other's penises and that MV1 asked him to perform oral sex on him, which FLORES said he subsequently did. When asked about the second occurrence of sexual contact with MV1, FLORES said they touched each other's penises and he performed oral sex on MV1. FLORES said MV1 did not ejaculate, but that he (FLORES) ejaculated on himself. FLORES admitted these instances of sexual contact occurred over the course of the three-week period prior to June 5, 2018.

28. On June 5, 2018, an HSI Forensic Interview Specialist (FIS) conducted and HSI special agent (SA) Justin Burnham witnessed an interview of MV1. During the interview, MV1 said he and FLORES had smoked marijuana or drank alcohol prior to the engagement of sexual activity. MV1 said FLORES used his hand to touch his penis and has performed oral sex on him within the past few weeks of his interview.

**d. Minor Victim 2 (Production/Distribution of Child Pornography):**

29. FLORES then described a time near the beginning of 2018 when he had engaged in a video-chat with an individual using Skype. FLORES said he was video chatting with this person in his bedroom at his residence located at 131 West 2<sup>nd</sup> Street in Dunkirk, New York. FLORES said he and MV2, a four-year-old girl, were in his bedroom and that they were laying on his bed while he was video chatting with this individual. The identity of



MV2 is known by law enforcement, but is being redacted from this affidavit because she is a minor. FLORES said MV2 was laying down on the bed in front of him watching the television which was further in front of her. FLORES said he and the man he was Skype chatting with were masturbating during the video chat while MV2 was watching television. When asked if MV2 was naked, FLORES said he just "pulling the shorts down a little bit". FLORES later clarified and said he pulled MV2's pants down below her butt cheeks and photographed her buttocks for this individual. FLORES said the individual he was communicating with told him "do this, do that" to MV2. FLORES said at one point, MV2 was on his lap. FLORES acknowledged that the individual he was communicating with over Skype probably asked him to put his hand down MV2's pants, but said that he just touched her stomach.

30. FLORES described another incident that occurred after the incident described in paragraph 17 above. FLORES said he had been drinking and was communicating over Skype with this same individual when this second event occurred. FLORES said he went downstairs to the kitchen where minor victim 2 (MV2) was sleeping on an air mattress. FLORES said he grabbed MV2's hand while she slept and put it on his penis while communicating with this individual over the internet. When asked if he masturbated himself with her hand, FLORES said that he did, that he photographed or video recorded the incident, and acknowledged the incident occurred sometime toward the end of 2017. FLORES said he didn't ejaculate while engaging in this behavior. FLORES said he engaged in these acts in order to please other men. When asked about the man he was

communicating with when he engaged in this behavior, FLORES said he met him on “Hangouts”, believed to be referring to Google Hangout.

31. On June 5, 2018, an HSI FIS attempted to interview MV2, but was unable to effectively communicate with her because of MV2’s young age.

32. During interviews conducted on June 5, 2018, FLORES provided verbal and written consent to assume his online identity and access stored information for the below social media accounts. In addition, FLORES provided HSI agents with any known passwords for these accounts.

- a. Google Hangouts associated with telephone number “(716) 467-2535”
- b. Hotmail account associated with “[dking\\_3@hotmail.com](mailto:dking_3@hotmail.com)”
- c. Tumbler account “dflo93”
- d. Gmail account [Parrotart@gmail.com](mailto:Parrotart@gmail.com)

**f. Preliminary Forensic Exam (Distribution/Receipt and Possession of Child**

**Pornography):**

33. During the aforementioned NYS search warrant, law enforcement officials discovered the cellular telephones referenced in paragraph 21 above that FLORES admitted were used to produce, distribute, receive, and possess child pornography. In June 2018, the information from these cellular telephones was extracted by an HSI computer forensic agent (CFA) and later reviewed by HSI SA Justin Burnham. During the review, SA Burnham

identified multiple images and videos of child pornography, including child pornography material involving toddlers. Examples of this child pornography include:

a. **“84578946786674385637485.mp4”** – This video file depicts the erect penis of an adult male being inserted into the anus of a pre-pubescent minor male child who appears to be under the age of ten years old. The focus of the recording device is on the insertion of the adult male penis so the upper body of the child is not visible. The child is hovering over the adult male who is lying on his back and the adult male is between the legs of the child.

b. **“67464.wmv”** – This video file depicts the erect penis of an adult male being inserted into the anus of a pre-pubescent minor male child who appears to be under the age of ten years old. The minor child is naked from the waist down, but appears to be wearing a green and white shirt. At points in the video, the minor child is seen on his hands and knees while the adult male stands behind him inserting his penis into the anus of the minor child.

c. **“5465.mp4”** – This video file depicts an adult male engaging in intercourse with a child that does not appear to be over the age of three. The adult male is wearing a red, long-sleeve shirt and what appears to be football pajama pants which are lowered during the video. The child is wearing a yellow top and appears to be naked from the waist down. At one point in the video, the adult man is seen inserting his erect penis into the anus of the pre-pubescent toddler child.

34. On March 6, 2016, a multimedia message service (MSM) message was sent from FLORES' cellular telephone to the contact of “Carlos” at telephone number (917) 485-

0076. The body of the message contained the text “Like this”. Attached to the MMS message was a file by the name of 2016-01-27-13-44-42-1.png. SA Burnham subsequently viewed this image file which depicted a naked, prepubescent minor male with his legs spread open while laying on top of a naked, adult male. The erect penis of the naked, adult male, who is also laying on his back, is seen inserted into the anus of the minor male. The genitals of the minor male are exposed to the recording device. At the bottom of the image, the following text can be seen: “DAD FUCK SON 0:23”.

**TECHNICAL BACKGROUND CONCERNING E-MAIL (Google & Microsoft)**

35. Based on my training and experience, including conversations with other law enforcement officers, I have learned that Google, Inc. and Microsoft Corporation provides a variety of on-line services, including electronic mail (“e-mail”) access, to the public. Google, Inc. allows subscribers to obtain e-mail accounts at the domain name of “google.com”, like the e-mail account listed in Attachment A, and Microsoft Corporation allows subscribers to obtain e-mail accounts at the domain names of “hotmail.com”, like the e-mail account listed in Attachment C. Subscribers obtain an account by registering with Google, Inc. or Microsoft Corporation, and during the registration process, both companies ask subscribers to provide basic personal information. Therefore, the computers of Google, Inc. and Microsoft Corporation are likely to contain stored electronic communications (including retrieved and unretrieved e-mail) for Google, Inc. and Microsoft Corporation subscribers and information concerning subscribers and their use of Google, Inc. and Microsoft Corporation services, such as account access information, e-mail transaction information, and account application information. In my training and experience, stored electronic communications such as email

may contain files, including contraband such as child pornography, as well as e-mail transaction information associated with these files which will likely show how these files were received and/or distributed to and from other individuals. All of the above information may constitute evidence of the crimes under investigation because the information can be used to identify instances of the production, distribution, receipt, and possession of child pornography as well as coercion/enticement. In addition this information can be used to identify the SUBJECT ACCOUNTS user or users as well as those users communicating with the SUBJECT ACCOUNTS who are also in violation of federal law.

36. Skype, a division of Microsoft Corporation, is used by individuals and businesses to make free video and voice calls, send instant messages, and share files with other people on Skype. Skype, which can be used on your mobile device, computer or tablet is free to download, but premium services can be purchased in order to call telephones and send short message service (SMS) messages. In my training and experience, individuals often times use Skype to engage in violations of the production, distribution, receipt, and possession of child pornography as well as the coercion/enticement of minors.

37. A Google, Inc. and Microsoft Corporation subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google, Inc. and Microsoft Corporation. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mail, including pictures and files.

38. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

39. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of that account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

40. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

41. As explained herein, information stored in connection with an e-mail account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an e-mail account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at the residence. For example, e-mail communications, contact lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the e-mail provider can show how and when the account was accessed or used. For example, as described below, e-mail providers typically log the Internet Protocol (IP) addresses from which users access the e-mail account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological context of the e-

mail account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the e-mail account owner's state of mind as it relates to the offense under investigation. For example, information in the e-mail account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

### TUMBLR

42. Tumblr is a microblogging and social networking website that allows users to post text and multimedia content. Users can make their posts public or private. Tumblr also allows users to communicate directly and privately, enabling them to share text communication, media and data files. This can include communications and media associated with the production, distribution, receipt and possession of child pornography as well as the enticement/coercion of minors.

43. In general, electronic communications service providers like Tumblr require subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, telephone numbers, e-mail addresses, and, for paying subscribers, a means and source of payment (including a credit or bank account number). Providers also typically retain certain



transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol (“IP”) address used to register the account and the IP addresses associated with particular log-ins to the account. Because every device that connects to the internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Tumblr account.

44. In some cases, Tumblr users will communicate directly with the provider about issues relating to their accounts, such as technical problems, billing inquiries, or complaints regarding other users. Providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well records of any actions taken by the provider or user as a result of the communications.

45. As referenced in paragraph 24 above, FLORES admitted he used social media companies, including Google e-mail and Google Voice, Microsoft Corporation e-mail and their division of Skype, as well as Tumblr, Inc. to distribute, receive, and possess child pornography, all in violation of federal law. In addition, Cybertips issued by Google, Inc. and Microsoft Corporation have shown that child pornography was uploaded to their accounts by a user at FLORES’ residence.

### **CONCLUSION**

46. Based upon the forgoing, the undersigned respectfully submits that there is probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 2251(a) (Production of Child Pornography), Title 18, United States Code, Section 2252A(a)(2)(A) (Distribution/Receipt of Child Pornography) and Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) as specifically described in Attachment B, Attachment D, and Attachment F to this application, are presently located within the SUBJECT ACCOUNTS. The undersigned therefore respectfully requests that the attached warrant be issued authorizing a search for the items listed in Attachment B, Attachment D, and Attachment F within the SUBJECT ACCOUNTS, which are more particularly described in Attachment A, Attachment C, and Attachment E to this application.

### **REQUEST FOR SEALING**

47. It is further respectfully requested that the Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left with the Custodian of Records associated with the SUBJECT ACCOUNTS). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and

premature disclosure of the contents of this affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.

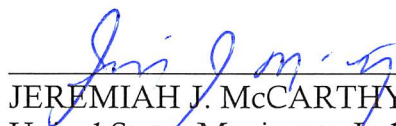


---

JUSTIN J. BURNHAM  
Special Agent  
Homeland Security Investigations

Sworn and subscribed to before

me this 16<sup>th</sup> day of July, 2018.



---

JEREMIAH J. McCARTHY  
United States Magistrate Judge

**ATTACHMENT A**

**PROPERTY TO BE SEARCHED**

The electronic mail account to be searched is a certain account controlled, owned, stored, or operated by the internet service provider known as Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043 in the Northern District of California. This warrant applies to information associated with the following e-mail accounts:

Email: Parrotart2012@gmail.com

Username: Parrotart2012

Account with Google Voice/Hangout Telephone Number: (716) 467-2535

**ATTACHMENT B**

**DESCRIPTION OF ITEMS TO BE SEIZED**

**I. Information to be disclosed by Google, Inc. (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc., regardless of whether such information is located within or outside of the United States, and including any e-mails, records, files, logs, or information that has been deleted but is still available to Google, Inc., Google, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of any and all e-mails stored in the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, attachments, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. Any deleted e-mails, including information described in subparagraph “a,” above;

c. The types of services utilized;

d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses

associated with session times and dates, account status, alternative e-mail addresses provided during registration, other Google accounts that share the same SMS or secondary email address as the target account as well as any other accounts that use the target email address as a secondary email address, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, Photos and Briefcase, and files;

f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

g. Any documents, folders, folder names and directory listing, images, data, videos and attachments stored within this account or accessible by the account. This would also include images, data, videos, documents, posts, and attachments stored in Google Picasa, Google+ including a copy of the Google+ profile and the Google+ Circles and Contacts, Google+ Photos, Google Earth, Google Docs, Google Calendar, Google Voice, Google Drive, Google Blogger, and Google Hangouts including and any other online storage accessible by a user associated with the accounts;

h. All date, time and IP Addresses for each uploaded and download file as well as all Share settings for Google Picasa, Google Docs, Google Drive, Google Blogger and any other online storage accessible through the account;

i. For the accounts in Attachment A, provide the Android device information, including IMEI/MEID, make and model, serial number, date and IP of last access to Google, and a list of all accounts that have ever been active on the device;

- j. All Google MAPS data from June of 2014 through the present associated with the account;
- k. All Google PHOTOS images, albums, videos, and all associated META or EXIF data related to the accounts listed in Attachment A. This shall include any uploaded images regardless if sent or received;
- l. All deleted, discarded, and trash folder photos, images, or thumbnail image files associated with the accounts listed in Attachment A;
- m. Any and all methods of payment provided by the subscriber to the provider for any premium services;
- n. Any and all Google, Inc. ID's listed on the subscriber's friends list; and
- o. All Google Hangouts data, including META or EXIF data, for all images, videos, messages, or incoming and outgoing calls;
- p. All previously preserved data in the account to include what is detailed in the paragraphs above.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 2251(a) (Production of Child Pornography), Title 18, United States Code, Section 2252A(a)(2)(A) (Distribution/Receipt of Child Pornography), and Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) that have been committed, including, for each account or identifier listed in Attachment A, information pertaining to the following matters:

- a. Communications, images, or videos related to the solicitation or production of images depicting child pornography and/or minors engaging in sexually explicit conduct;
- b. Evidence of the possession, receipt, production or distribution of images depicting child pornography and/or minors engaging in sexually explicit conduct;
- c. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts; and
- d. Communications, images, or videos related to the enticement of minors.



**ATTACHMENT C**

**PROPERTY TO BE SEARCHED**

The electronic mail account to be searched is a certain account controlled, owned, stored, or operated by the internet service provider known as Microsoft Corporation, an internet portal and electronic mail company headquartered at 1 Microsoft Way in Redwood, Washington 98052. This warrant applies to information associated with the following Microsoft accounts:

Microsoft account associated with Email: dking\_3@hotmail.com

Microsoft account associated with username: dking\_3

Microsoft account associated with Skype Username: dflores93

Microsoft account associated with Skype Username: dfloresart

**ATTACHMENT D**

**DESCRIPTION OF ITEMS TO BE SEIZED**

**I. Information to be disclosed by Microsoft Corporation (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment C:

- a. The contents of any and all e-mails stored in the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, attachments, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. Any deleted e-mails, including information described in subparagraph “a,” above;
- c. The types of services utilized;
- d. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided

during registration, other Provider accounts that share the same SMS or secondary email address as the target account as well as any other accounts that use the target email address as a secondary email address, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, Photos and Briefcase, and files;

f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

g. Any documents, folders, folder names and directory listing, images, data, videos and attachments stored within this account or accessible by the account.

h. All date, time and IP Addresses for each uploaded and download file as well as all share settings for the Providers cloud storage and any other online storage accessible by the accounts listed in Attachment C;

i. For the accounts in Attachment C, provide the MAC address and/or Android device information, including IMEI/MEID, make and model, serial number, date and IP of last access to the Provider, and a list of all accounts that have ever been active on the device;

j. All records, including the content of communications, pertaining to chats or Provider communications and exchanges between the accounts listed in Attachment C and other Provider users;

k. All deleted, discarded, and trash folder photos, images, or thumbnail image files associated with the accounts listed in Attachment C;

m. Any and all methods of payment provided by the subscriber to the Provider for any premium services;

o. All previously preserved data in the account to include what is detailed in the paragraphs above.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 2251(a) (Production of Child Pornography), Title 18, United States Code, Section 2252A(a)(2)(A) (Distribution/Receipt of Child Pornography), and Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) that have been committed, including, for each account or identifier listed in Attachment C, information pertaining to the following matters:

a. Communications, images, or videos related to the solicitation or production of images depicting child pornography and/or minors engaging in sexually explicit conduct;

b. Evidence of the possession, receipt, production or distribution of images depicting child pornography and/or minors engaging in sexually explicit conduct;

c. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts; and

d. Communications, images, or videos related to the enticement of minors.

**ATTACHMENT E**

**PROPERTY TO BE SEARCHED**

The account to be searched is a microblogging and social networking company controlled by Tumblr, Inc., a company headquartered in New York, New York. The account name to be searched belongs to the following Tumblr user:

Username: dflo93

**ATTACHMENT F**

**DESCRIPTION OF ITEMS TO BE SEIZED**

**I. Information to be disclosed by Tumblr, Inc. (the “Provider”)**

To the extent that the information described in Attachment E is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any forms of communication, including e-mails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment E:

- a. The types of services utilized;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, other Provider accounts that have used the email address listed in Attachment E, methods of connecting, log files, and means and source of payment (including any credit or bank account number) including payment for premium services;
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, videos or other files;
- d. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

- e. Any documents, folders, folder names and directory listing, images, data, videos and attachments stored within this account or accessible by the account.
- f. All date, time and IP Addresses for each uploaded and download file and any other online storage accessible by the accounts listed in Attachment E;
- g. For the accounts in Attachment E, provide the MAC address or Android device information, including IMEI/MEID, make and model, serial number, date and IP of last access to the Provider, and a list of all accounts that have ever been active on the device;
- h. All records, including the content of communications, pertaining to chats, messaging or other communications involving the accounts listed in Attachment E;
- i. All deleted, discarded, and trash folder photos, images, or thumbnail image files associated with the accounts listed in Attachment E;
- j. All previously preserved data in the account to include what is detailed in the paragraphs above.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Section 2251(a) (Production of Child Pornography), Title 18, United States Code, Section 2252A(a)(2)(A) (Distribution/Receipt of Child Pornography), and Title 18, United States Code, Section 2252A(a)(5)(B) (Possession of Child Pornography) that have been committed, including, for each account or identifier listed in Attachment E, information pertaining to the following matters:

- a. Communications, images, or videos related to the solicitation or production of images depicting child pornography and/or minors engaging in sexually explicit conduct;
- b. Evidence of the possession, receipt, production or distribution of images depicting child pornography and/or minors engaging in sexually explicit conduct;
- c. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts; and
- d. Communications, images, or videos related to the enticement of minors.